4/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent WPI

012591177 **Image available**
WPI Acc No: 1999-397283/199934
XRPX Acc No: N99-297154
Encryption strength evaluation support apparatus
Patent Assignee: NEC CORP (NIDE)
Inventor: TSUNOO Y
Number of Countries: 027 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 932272	A2	19990728	EP 99101386	A	19990126	199934	B
JP 11212452	A	19990806	JP 9829132	A	19980127	199942	
CA 2259873	A1	19990727	CA 2259873	A	19990122	200003	

Priority Applications (No Type Date): JP 9829132 A 19980127
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 932272	A2	E	35	H04L-009/00	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
CA 2259873	A1	E		G06F-017/18	
JP 11212452	A		21	G09C-001/00	

Abstract (Basic): EP 932272 A2
NOVELTY - The apparatus is capable of evaluatingencryption strength independent of any specific decodingmethod and finely analyzing the behaviour of encryptionconversion.
DETAILED DESCRIPTION - The apparatus includes astatistical data sampling program executing mechanism forstatistically obtaining correlations between individual bitsof input and output data of an encryption device to beevaluated. The apparatus also includes a statistical resultstorage mechanism for storing the bit correlations obtainedby the statistical data sampling program executing mechanism.A statistical result edit and output mechanism is included toedit and output the bit correlations stored in the statisticalresult store in the form of a table or a two or threedimensional graph.
USE - The apparatus is used to evaluate the encryptionstrength of an encryption device.
ADVANTAGE - In the apparatus the correlations betweenindividual bits of input and output data can be displayed asvarious graphs such as 3D contour graph. Consequently, detailsof the behaviour of encryption conversion can be finely andextremely easily analyzed. This allows accurate evaluationfeasible.
DESCRIPTION OF DRAWING(S) - The drawing shows the whole configuration of the encryption strengthevaluation support apparatus.
pp; 35 DwgNo 1/18
Title Terms: ENCRYPTION; STRENGTH; EVALUATE; SUPPORT; APPARATUS
Derwent Class: W01
International Patent Class (Main): G06F-017/18; G09C-001/00; H04L-009/00
File Segment: EPI

4/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

06270864 **Image available**
CRYPTOGRAPHIC ROBUSTNESS EVALUATION SUPPORT DEVICE AND MACHINE READABLE RECORD MEDIUM RECORDED WITH PROGRAM

PUB. NO.: 11-212452 A]
PUBLISHED: August 06, 1999 (19990806)
INVENTOR(s): SUMIO YUKIYASU
APPLICANT(s): NEC CORP
APPL. NO.: 10-029132 [JP 9829132]
FILED: January 27, 1998 (19980127)

INTL CLASS: G09C-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To provide a cryptographic robustness evaluation support device which finely and easily recognizes behaviors of encryption conversion.

SOLUTION: An evaluation object data group generation means 101 generates an evaluation object data group including an evaluation object program, evaluation conditions, etc. A statistical program library generation means 102 generates a library of various statistical programs. A statistical data pick-up program execution means 104 takes the evaluation object data group and statistical programs as the input to generate and execute a program which statistically obtains the correlations of individual bits of input/output data of a cipher device as an evaluation object and stores statistically obtained data in a statistical result storage means 106. A statistical result editing and output means 105 edits correlations of individual bits stored in the statistical result storage means 106 into a form of a table or a two-dimensional or three-dimensional graph and outputs it.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－212452

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６１０	Ｇ０９Ｃ　1/00	６１０Ｚ

審査請求　有　　請求項の数８　ＦＤ　（全 21 頁）

(21)出願番号　特願平10－29132

(22)出願日　平成10年(1998)１月27日

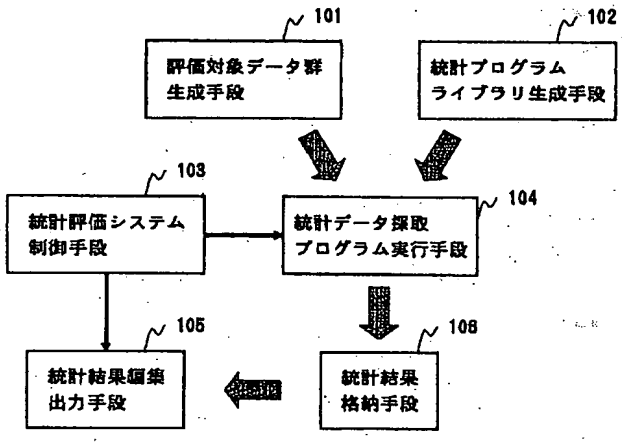
(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　角尾　幸保
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　弁理士　境　廣巳

(54)【発明の名称】　暗号強度評価支援装置及びプログラムを記録した機械読み取り可能な記録媒体

(57)【要約】

【課題】　暗号化変換の挙動をきめ細かく容易に把握できる暗号強度評価支援装置を提供する。

【解決手段】　評価対象データ群生成手段101 は評価対象プログラムや評価条件等を含む評価対象データ群を生成する。統計プログラムライブラリ生成手段102は各種の統計プログラムのライブラリを生成する。統計データ採取プログラム実行手段104 は、評価対象データ群及び統計プログラムを入力し、評価対象となる暗号装置の入出力データのビットごとの相関関係を統計的に求めるプログラムを生成して実行し、統計的に求めたデータを統計結果格納手段106 に格納する。統計結果編集出力手段105 は、統計結果格納手段106 に格納されたビットごとの相関関係を表形式または２次元若しくは３次元のグラフ形式に編集して出力する。



1

【特許請求の範囲】

【請求項１】　評価対象となる暗号装置の入出力データのビットごとの相関関係を統計的に求める統計データ採取プログラム実行手段と、

前記統計データ採取プログラム実行手段により求められたビットごとの相関関係を格納する統計結果格納手段と、

前記統計結果格納手段に格納されたビットごとの相関関係を表形式または２次元若しくは３次元のグラフ形式に編集して出力する統計結果編集出力手段とを備えることを特徴とする暗号強度評価支援装置。

【請求項２】　評価対象となる暗号プログラムを作成するための評価対象プログラム作成手段を備え、

前記統計データ採取プログラム実行手段は前記評価対象プログラム作成手段で作成された評価対象プログラムの入出力データのビットごとの相関関係を統計的に求めることを特徴とする請求項１記載の暗号強度評価支援装置。

【請求項３】　所定の評価項目ごとにその評価項目の評価に必要なデータを計算する統計プログラムを保持する統計プログラムライブラリと、

評価対象となる暗号プログラムを作成するための評価対象プログラム作成手段，評価条件を設定するための評価条件設定手段および前記評価対象プログラム作成手段で作成された評価対象プログラムと前記統計プログラムとのインタフェースを設定するインタフェース関数設定手段を有し、前記作成された評価対象プログラム，前記設定された評価条件およびインタフェースから構成される評価対象データ群を保持する評価対象データ群生成手段とを備え、

前記統計データ採取プログラム実行手段は、前記評価対象データ群と前記統計プログラムライブラリ中の統計プログラムとから評価対象プログラムの入出力データのビットごとの相関関係を統計的に求める統計データ採取プログラムを生成する統計データ採取プログラム生成・起動（再開）手段を含むことを特徴とする請求項１記載の暗号強度評価支援装置。

【請求項４】　加算，減算，論理演算等の基本機能をライブラリ化してある基本機能ライブラリと、該基本機能ライブラリの基本機能を使って統計プログラムライブラリに新規に追加すべき統計プログラムを作成するための統計プログラムライブラリ生成手段とを備えることを特徴とする請求項３記載の暗号強度評価支援装置。

【請求項５】　前記統計データ採取プログラム実行手段は、複数の評価項目についての統計データを順次に収集する構成を有することを特徴とする請求項１，２，３または４記載の暗号強度評価支援装置。

【請求項６】　前記統計データ採取プログラム実行手段は、利用者からの指示に従って現在処理中の評価項目の処理を中断して次の評価項目を処理する機能を備えることを特徴とする請求項５記載の暗号強度評価支援装置。

2

【請求項７】　前記統計データ採取プログラム実行手段は、利用者からの指示に従って中断した評価項目の処理を再開する機能を備えることを特徴とする請求項６記載の暗号強度評価支援装置。

【請求項８】　コンピュータを、

評価対象となる暗号装置の入出力データのビットごとの相関関係を統計的に求める統計データ採取プログラム実行手段、

前記統計データ採取プログラム実行手段により求められたビットごとの相関関係を格納する統計結果格納手段、

前記統計結果格納手段に格納されたビットごとの相関関係を表形式または２次元若しくは３次元のグラフ形式に編集して出力する統計結果編集出力手段、

として機能させるプログラムを記録した機械読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、統計的な手法を用いて暗号装置の暗号強度を評価するのに好適な暗号強度評価支援装置に関する。

【０００２】

【従来の技術】暗号アルゴリズムの強度を評価する従来の技術は、特定の解読法に基づくものと統計的手法に基づくものとに大別される。

【０００３】特定の解読法に基づく暗号強度評価の例には、特開平８－１９０３４４号公報記載の「暗号アルゴリズムの強度評価方法及び強度評価装置」及びそれに類似する特開平９－１６０４８９号公報記載の「暗号性能評価装置」がある。これらは、いずれもブロック暗号に対する線形解読法に対する強度をもって暗号アルゴリズムの強度とするものである。即ち、前者は強度評価を行う暗号アルゴリズムから構成し得る最大の偏差率をもつ線形近似式を探索し、この結果から暗号アルゴリズムの線形解読法に対する強度を定量的に評価しようとしており、後者は線形解読法における線形相関の検出効率をあげて評価の性能を向上させようとするものである。なお、線形解読法の詳細は、松井充「ＤＥＳ暗号の線形解読法（１）」、ＳＣＩＳ９３－３Ｃ，（Ｊａｎ，１９９３）に記載されている。

【０００４】他方、統計的な手法に基づく従来の暗号強度評価は、例えば「暗号と情報セキュリティ」（１９９０年３月２９日，昭晃堂発行）の『２．５　暗号文ランダム性評価指標』（ｐ．４９～ｐ．５６）に記載されるように、入出力データ間の相関の最大値，平均値，分散などの数値によって暗号強度を評価しようとするものである。また、同文献には、複数の暗号アルゴリズムの強度の優劣を前記数値の比較によって判定する点も記載されている。

【０００５】

【発明が解決しようとする課題】特定の解読法に基づく暗号強度評価では、線形解読法という特定の解読法に依存するため、その解読法が適用可能でない暗号アルゴリズムに対する強度評価は原理的に不可能であり、汎用性に乏しい。これに対して統計的な手法によって暗号強度を評価する手法は、特定の解読法に依存しない為、より汎用性が高いと言える。

【０００６】しかしながら、統計的な手法による従来の暗号強度評価技術は、入出力データ間の相関の最大値，平均値，分散などの数値で評価している。これらの数値は多数の標本値の代表値であるため、暗号化変換の挙動をきめ細かく把握することができず、場合によっては評価を誤る危険性がある。

【０００７】そこで本発明の目的は、特定の解読法に依存しないで暗号強度の評価が行え、然も暗号化変換の挙動をきめ細かく把握できる暗号強度評価支援装置を提供することにある。

【０００８】また本発明の別の目的は、暗号化変換の挙動を容易に把握することができる暗号強度評価支援装置を提供することにある。

【０００９】

【課題を解決するための手段】本発明は上記の目的を達成するために、評価対象となる暗号装置の入出力データのビットごとの相関関係を統計的に求める統計データ採取プログラム実行手段（図１の１０４）と、前記統計データ採取プログラム実行手段により求められたビットごとの相関関係を格納する統計結果格納手段（図１の１０６）と、前記統計結果格納手段に格納されたビットごとの相関関係を表形式または２次元若しくは３次元のグラフ形式に編集して出力する統計結果編集出力手段（図１の１０５）とを備えている。

【００１０】このように構成された暗号強度評価支援装置にあっては、統計データ採取プログラム実行手段が、評価対象となる暗号装置の入出力データのビットごとの相関関係を統計的に求めて統計結果格納手段に格納し、統計結果編集出力手段が、統計結果格納手段に格納されたビットごとの相関関係を表形式または２次元若しくは３次元のグラフ形式に編集して出力することにより、特定の解読法に依存しないで暗号強度の評価が行えるようにすると共に、暗号化変換の挙動をきめ細かく容易に把握できるようにする。

【００１１】また本発明は、評価対象となる暗号プログラムを作成するための評価対象プログラム作成手段（図２の２０１）を備え、前記統計データ採取プログラム実行手段は前記評価対象プログラム作成手段で作成された評価対象プログラムの入出力データのビットごとの相関関係を統計的に求めることを特徴とする。これによって、暗号アルゴリズムの設計と評価が同一の装置で実施でき、開発の効率が向上する。

【００１２】また本発明は、所定の評価項目ごとにその

評価項目の評価に必要なデータを計算する統計プログラムを保持する統計プログラムライブラリ（図３の３０３）と、評価対象となる暗号プログラムを作成するための評価対象プログラム作成手段（図２の２０１），評価条件を設定するための評価条件設定手段（図２の２０３）および前記評価対象プログラム作成手段で作成された評価対象プログラムと前記統計プログラムとのインタフェースを設定するインタフェース関数設定手段（図２の２０２）を有し、前記作成された評価対象プログラム，前記設定された評価条件およびインタフェースから構成される評価対象データ群を保持する評価対象データ群生成手段（図１の１０１）とを備え、前記統計データ採取プログラム実行手段は、前記評価対象データ群と前記統計プログラムライブラリ中の統計プログラムとから評価対象プログラムの入出力データのビットごとの相関関係を統計的に求める統計データ採取プログラムを生成する統計データ採取プログラム生成・起動（再開）手段（図４の４０５）を含むことを特徴とする。これによって、暗号アルゴリズムの設計と予め統計プログラムライブラリに保持された統計プログラムを利用した評価とを同一の装置で実施でき、開発の効率が向上する。

【００１３】また本発明は、加算，減算，論理演算等の基本機能をライブラリ化してある基本機能ライブラリ（図３の３０２）と、該基本機能ライブラリの基本機能を使って統計プログラムライブラリに新規に追加すべき統計プログラムを作成するための統計プログラムライブラリ生成手段（図３の３０１）とを備えることを特徴とする。これによって、利用者は任意の統計プログラムを自由に作成でき、それを用いた評価が行える。

【００１４】また本発明は、前記統計データ採取プログラム実行手段が、複数の評価項目についての統計データを順次に収集する構成を有する。これによって、複数の評価項目を一括して評価することができる。

【００１５】また本発明は、前記統計データ採取プログラム実行手段が、利用者からの指示に従って現在処理中の評価項目の処理を中断して次の評価項目を処理する機能や、利用者からの指示に従って中断した評価項目の処理を再開する機能を備えることを特徴とする。

【００１６】

【発明の実施の形態】次に本発明の実施の形態の例について図面を参照して詳細に説明する。

【００１７】図１を参照すると、本発明の暗号強度評価支援装置の実施の形態は、評価対象データ群生成手段１０１と、統計プログラムライブラリ生成手段１０２と、統計評価システム制御手段１０３と、統計データ採取プログラム実行手段１０４と、統計結果編集出力手段１０５と、統計結果格納手段１０６とを有する。

【００１８】統計プログラムライブラリ生成手段１０２は、所定の評価項目ごとに、その評価項目の評価に必要なデータを計算する統計プログラムをライブラリ化して

ある統計プログラムライブラリを有している。また、評価担当者自身が任意の統計プログラムを作成できるような支援機能を有している。ここで、統計評価項目としては、例えばビットバランス，出力ビット間関連，入出力ビット間関連，アバランシュなどがある（各項目の詳細については後述する）。

【００１９】評価対象データ群生成手段１０１は、暗号強度を評価しようとする評価対象プログラムと、その評価条件と、評価対象プログラムと統計プログラムとのインタフェースとを含む評価対象データ群を有している。また、評価担当者自身が評価対象の暗号アルゴリズムや評価条件などを任意に作成できるような支援機能を有している。

【００２０】統計データ採取プログラム実行手段１０４は、評価対象データ群生成手段１０１から評価対象データ群を入力すると共に、その評価項目の評価に必要なデータを計算する統計プログラムを統計プログラムライブラリ生成手段１０２の統計プログラムライブラリから入力し、これらから、評価対象となる暗号アルゴリズムの入出力データのビットごとの相関関係を統計的に求める統計データ採取プログラムを生成し、実行する機能を有している。

【００２１】統計結果格納手段１０６は、統計データ採取プログラム実行手段１０４で採取された暗号アルゴリズムの入出力データのビットごとの相関関係の統計結果を格納する手段である。

【００２２】統計結果編集出力手段１０５は、統計結果格納手段１０６に格納されたビットごとの相関関係を表形式または２次元若しくは３次元のグラフ形式に編集して出力する手段である。

【００２３】統計評価システム制御手段１０３は、評価担当者からの各種の指示を受け、その指示内容に従って統計データ採取プログラム実行手段１０４および統計結果編集出力手段１０５の実行を制御する手段である。

【００２４】以上のように構成された本実施の形態の暗号強度評価支援装置にあっては、評価担当者が、統計プログラムライブラリ生成手段１０２中に統計プログラムライブラリを準備すると共に、評価対象データ群生成手段１０１中に、評価対象とするプログラム，どのような評価項目の評価を行うか等の評価条件，及び評価対象プログラムと必要な統計プログラムとのインタフェースとを記述した評価対象データ群を用意した後、統計データの採取を指示すると、統計評価システム制御手段１０３からの指示に従って統計データ採取プログラム実行手段１０４が、評価対象データ群と統計プログラムライブラリとに基づいて統計データ採取プログラムを生成して実行することにより、評価対象となる暗号アルゴリズムの入出力データのビットごとの相関関係を統計的に求めて統計結果格納手段１０６に格納する。そして、評価担当者が統計結果の編集出力を指示すると、統計評価システム制御手段１０３からの指示に従って統計結果編集出力手段１０５が、統計結果格納手段１０６に格納された統計結果を表形式または２次元若しくは３次元のグラフ形式に編集して出力する。これにより、評価担当者は評価対象となる暗号アルゴリズムの暗号化変換の挙動をきめ細かく且つ容易に把握することができる。

【００２５】以下、本実施の形態の暗号強度評価支援装置における各部の構成例とその動作について詳細に説明する。

【００２６】図２は評価対象データ群生成手段１０１の構成例を示すブロック図、図３は統計プログラムライブラリ生成手段１０２の構成例を示すブロック図である。

【００２７】まず図３を参照すると、統計プログラムライブラリ生成手段１０２の一例は、加算，減算，論理演算，平均計算などの基本的な演算機能を基本機能としてライブラリ化してある基本機能ライブラリ３０２と、この基本機能ライブラリ３０２に用意された基本機能を使って統計プログラムを作成する環境を評価担当者に提供する統計プログラムライブラリ生成手段３０１と、この統計プログラムライブラリ生成手段３０１で生成された統計プログラムを格納する統計プログラムライブラリ３０３とで構成されている。

【００２８】ここで、統計プログラムとは、評価対象となる暗号アルゴリズムの入力となる平文及び鍵を評価データとして生成し、この評価データを評価対象の暗号アルゴリズムに入力したときに得られる出力の暗号文や前記評価データから統計データを計算する処理を実行するプログラムであり、各評価項目ごとに用意される。以下、幾つかの代表的な評価項目について、評価項目の内容とそれに必要な統計プログラムの機能を説明する。なお、評価対象アルゴリズムをＦ、平文をＭ、鍵をＫ、評価対象アルゴリズムの出力をＦ（Ｍ，Ｋ）、入力のビット幅をｎ、出力のビット幅をｍとする。

【００２９】○アバランシュ性評価；アバランシュ性評価とは、入力データに１ビットの変化を与えたとき、出力ビットにどれだけ波及するかを評価するもので、例えば次の手順で評価する。

（１）Ｍを乱数で生成する。

（２）Ｆ（Ｍ，Ｋ）を求める。

（３）Ｍの第ｉビットを１ビット反転したデータM_iを作成する。

（４）Ｆ（M_i，Ｋ）を求める。

（５）Ｆ（Ｍ，Ｋ）ｘｏｒＦ（M_i，Ｋ）の第ｊビットが０ならば－１を、１ならば１を、ｎ行ｍ列の二次元配列Ａの要素A_{ij}に加算する（ｘｏｒ；排他的論理和）

（６）多数のＭ，Ｋについて（１）～（５）を繰り返す。これにより、Ａの各要素には、特定の入力ビットを反転した場合の、特定の出力ビットの［反転回数－非反転回数］が格納され、それがアバランシュデータとなる。

アバランシュ性評価用の統計プログラムでは、上記の手順のうち、多数のM，Kを乱数で生成する処理、Mの１ビットを反転したM_iを作成する処理、F（M，K）ｘｏｒF（M_i，K）の結果に基づきAを更新する処理を担い、F（M，K）やF（M_i，K）を求める処理は評価対象プログラムが担う。なお、統計プログラムで生成された評価データの評価対象プログラムへの引き渡しや、評価対象プログラムで生成されたデータの統計プログラムへの引き渡しなどは、評価対象データ群中の評価対象プログラムと統計プログラムとのインタフェースに従って行われる。これは以下の評価項目でも同じである。

【００３０】○入出力ビット間関連性評価

入出力ビット間関連性評価とは、入力データの各ビットと出力データの各ビットとの関連性を評価するものであり、例えば次の手順で評価する。

（１）Mを乱数で生成する。

（２）F（M，K）を求める。

（３）Mの各ビットｉ毎に、F（M，K）の各ビットｊとの排他的論理和をとり、０ならば－１を、１ならば１を、ｎ行ｍ列の二次元配列Aの要素A_{ij}に加算する。

（４）多数のM，Kについて（１）～（３）を繰り返す。これにより、Aの各要素には、特定の入力ビットと特定の出力ビットとの［不一致回数－一致回数］が格納され、それが入出力ビット間関連性データとなる。

入出力ビット間関連性評価用の統計プログラムでは、上記の手順のうち、多数のM，Kを乱数で生成する処理、Mの各ビット毎にF（M，K）の各ビットと排他的論理和をとってAを更新する処理を担い、F（M，K）を求める処理は評価対象プログラムが担う。

【００３１】○出力ビット間関連性評価

出力ビット間関連性評価とは、出力データの各ビット間の関連性を評価するものであり、例えば次の手順で評価する。

（１）Mを乱数で生成する。

（２）F（M，K）を求める。

（３）F（M，K）の各ビットｉ毎に、F（M，K）の他のビットｊとの排他的論理和をとり、０ならば－１を、１ならば１を、ｍ行ｍ列の二次元配列Aの要素A_{ij}に加算する。

（４）多数のM，Kについて（１）～（３）を繰り返す。これにより、Aの各要素には、特定の出力ビットと特定の出力ビットとの［不一致回数－一致回数］が格納され、それが出力ビット間関連性データとなる。

出力ビット間関連性評価用の統計プログラムでは、上記の手順のうち、多数のM，Kを乱数で生成する処理、F（M，K）の各ビット毎にF（M，K）の他のビットｊとの排他的論理和をとってAを更新する処理を担い、F（M，K）を求める処理は評価対象プログラムが担う。

【００３２】○ビットバランス性評価

ビットバランス性評価とは、出力データの各ビットごとの１，０の出現頻度を評価するものであり、例えば次の手順で評価する。

（１）Mを乱数で生成する。

（２）F（M，K）を求める。

（３）F（M，K）の各ビットｉ毎に、０ならば－１を、１ならば１を、ｍ行の一次元配列Bの要素B_iに加算する。

（４）多数のM，Kについて（１）～（３）を繰り返す。これにより、Bの各要素には、特定の出力ビットの［１出現数－０出現数］が格納され、それがビットバランスデータとなる。

ビットバランス性評価用の統計プログラムでは、上記の手順のうち、多数のM，Kを乱数で生成する処理、F（M，K）の各ビット毎の値によりBを更新する処理を担い、F（M，K）を求める処理は評価対象プログラムが担う。

【００３３】以上のような種々の統計プログラムの作成を支援する統計プログラムライブラリ生成手段３０１は、基本機能ライブラリ３０２を含めて、例えばＭｉｃｒｏｓｏｆｔ　Ｖｉｓｕａｌ　C++ 4.2で実現することができる。統計プログラムライブラリ３０３中に適当な統計プログラムが存在しない場合、評価担当者は、統計プログラムライブラリ生成手段３０１が提供する環境の下で、基本機能ライブラリ３０２中の加算，減算，論理演算，平均計算等の基本的な演算機能を使って所望の統計プログラムを作成し、統計プログラムライブラリ３０３に追加しておくことが可能である。

【００３４】次に図２を参照すると、評価対象データ群生成手段１０１の一例は、評価対象プログラム作成手段２０１と、インタフェース関数設定手段２０２と、評価条件設定手段２０３と、評価対象データ群２０４とを有している。

【００３５】評価対象プログラム作成手段２０１は、評価対象プログラムを作成する環境を評価担当者に提供する手段である。

【００３６】評価条件設定手段２０３は、評価対象プログラムに対してどのような評価項目の評価を行うか、鍵やデータの幅を幾らにするか等の評価条件を設定する環境を評価担当者に提供する手段である。

【００３７】インタフェース関数設定手段２０２は、評価対象プログラムと統計プログラムとのインタフェースを設定する環境を、評価担当者に提供する手段である。前述の評価項目の説明箇所で触れたように、評価対象プログラムについて評価する場合、統計プログラムを使用するが、評価対象プログラムと統計プログラムとは別個に作成されるため、両者間のデータ引き渡しなどのインタフェースを定めておく必要がある。インタフェース関数設定手段２０２はそのようなインタフェースを評価担当者が作成するための手段である。

【００３８】以上の評価対象プログラム作成手段２０

１，インタフェース関数設定手段２０２および評価条件設定手段２０３は、例えばＭｉｃｒｏｓｏｆｔ　Ｖｉｓｕａｌ Ｃ++ 4.2で実現することができる。

【００３９】評価対象データ群２０４は、評価対象プログラム作成手段２０１で作成された評価対象プログラムと、インタフェース関数設定手段２０２で設定されたインタフェースと、評価条件設定手段２０３で設定された評価条件とを合わせたものであり、統計データ採取プログラム実行手段１０４の入力となる。

【００４０】このように図２の評価対象データ群生成手段１０１にあっては、暗号強度評価支援装置自体に評価対象プログラム作成手段２０１を持たせているため、暗号プログラムの設計→評価→修正→再評価といった一連の作業を効率良く実施することができる。また、インタフェース関数設定手段２０２および評価条件設定手段２０３を有するため、作成した評価対象プログラムに対して任意の評価項目の評価が可能である。

【００４１】図４は統計データ採取プログラム実行手段１０４の構成例を示すブロック図、図５は統計結果編集出力手段１０５の構成例を示すブロック図、図６は統計評価システム制御手段１０３の動作例を示すフローチャート、図７乃至図１０は統計データ採取プログラム実行手段１０４中の各手段の動作例を示すフローチャートである。以下、これらの図を参照して残りの構成要素について説明する。

【００４２】まず図６を参照すると、統計評価システム制御手段１０３は、動作を開始すると（ステップ６０１）、操作員の入力監視を行う（ステップ６０２）。この操作員の入力監視により検出される入力信号は、以降で説明する制御の指示ができるならば、どのような入力形態でもかまわない。例えば、操作員のキーボード入力でも良いし、新規に準備した操作パネルからの入力でも良いし、何らかの制御プログラムからの制御信号の通知でも良い。

【００４３】ステップ６０２で、操作員からの入力が検出された場合、その入力による制御の指示内容を判定する（ステップ６０３，６０５，６０７）。操作員から入力される制御の指示は、統計データ採取に関連する指示と、統計結果の編集出力に関連する指示と、統計評価システム制御手段１０３自身の終了指示とに大別される。また、操作員から入力される統計データ採取に関連する指示には、採取の開始（再開）指示と採取の中断指示とがある。

【００４４】制御指示が統計データ採取に関連する指示であるときは（ステップ６０３でＹＥＳ）、統計データ採取プログラム実行手段１０４に制御データを通知し（ステップ６０４）、操作員の入力監視ステップ６０２に戻る。このとき、操作員から入力される統計データ採取に関連する指示が、採取の開始（再開）指示のときにはデータ採取開始の指示を示す制御データを、また、採取の中断指示のときはデータ採取終了の指示を示す制御データを、それぞれ統計データ採取プログラム実行手段１０４に通知する。

【００４５】制御指示が統計結果の編集出力に関連する指示であるときは（ステップ６０５でＹＥＳ）、統計結果編集出力手段１０５に制御データを通知し（ステップ６０６）、操作員の入力監視ステップ６０２に戻る。

【００４６】制御指示が統計評価システム制御手段１０３自身の終了指示であるときは（ステップ６０７でＹＥＳ）、プログラム動作の終了の指示を示す制御データを統計データ採取プログラム実行手段１０４に通知する等の必要な終了処理を行って自身を終了する（ステップ６０８）。

【００４７】次に図４を参照すると、統計データ採取プログラム実行手段１０４の一例は、統計データ採取プログラム動作監視手段４０３と、統計データ採取プログラム中断・終了処理実行手段４０４と、統計データ採取プログラム生成・起動（再開）手段４０５と、統計データ採取プログラム４０６とを有している。統計データ採取プログラム生成・起動（再開）手段４０５は、統計データ採取プログラム動作監視手段４０３からの制御を受け、統計データ採取プログラム４０６を生成したり、その起動（再開）処理を実行する手段である。統計データ採取プログラム中断・終了処理実行手段４０４は、統計データ採取プログラム動作監視手段４０３からの制御を受け、統計データ採取プログラム４０６を中断したり、その終了処理を実行する手段である。統計データ採取プログラム動作監視手段４０３は、統計評価システム制御手段１０３からの制御および統計データ採取プログラム４０６からの終了通知を受け、統計データ採取プログラム生成・起動（再開）手段４０５および統計データ採取プログラム中断・終了処理実行手段４０４を制御して、統計データ採取プログラムの実行を制御する手段である。

【００４８】図７を参照すると、統計データ採取プログラム動作監視手段４０３は、動作を開始すると（ステップ７０１）、ステップ７０２～７０８の動作を実行する。まず動作開始後、統計評価システム制御手段１０３からの制御データ受信待ちを行い（ステップ７０２）、制御データを検出したら制御の指示内容を判定する（ステップ７０３，７０５，７０７）。統計評価システム制御手段１０３から送信される制御データには、データ採取開始を指示する制御データ、データ採取終了を指示する制御データ、プログラム動作の終了を指示する制御データがある。

【００４９】統計評価システム制御手段１０３からの制御データがデータ採取開始の指示であるときは（ステップ７０３でＹＥＳ）、統計データ採取プログラム生成・起動（再開）手段４０５に制御データを通知し（ステップ７０４）、統計評価システム制御手段１０３からの制

御データ受信待ちステップ７０２に戻る。ステップ７０４では、統計データ採取プログラム４０６が未生成のときは、統計データ採取プログラムの生成指示を示す制御データを出し、統計データ採取プログラム４０６が生成済のときは、統計データ採取プログラムの起動指示を示す制御データを出す。

【００５０】統計評価システム制御手段１０３からの制御データがデータ採取終了の指示であるときは（ステップ７０５でＹＥＳ）、統計データ採取プログラム中断・終了処理実行手段４０４に対して統計データ採取プログラム４０６の中断を指示する制御データを出し（ステップ７０６）、統計評価システム制御手段１０３からの制御データ受信待ちステップ７０２に戻る。

【００５１】統計評価システム制御手段１０３からの制御データがプログラム動作の終了指示であるときは（ステップ７０７でＹＥＳ）、統計データ採取プログラム生成・起動（再開）手段４０５及び統計データ採取プログラム中断・終了処理実行手段４０４に対してプログラム動作の終了を指示する制御データを通知する等の終了処理を実施した後、統計データ採取プログラム４０６からの終了通知を待って自身を終了する（ステップ７０８）。

【００５２】図８を参照すると、統計データ採取プログラム生成・起動（再開）手段４０５は、動作を開始すると（ステップ８０１）、ステップ８０２～８０８の動作を実行する。まず動作開始後、統計データ採取プログラム動作監視手段４０３からの制御データ受信待ちを行い（ステップ８０２）、制御データを検出したら制御の指示内容を判定する（ステップ８０３，８０５，８０７）。統計データ採取プログラム動作監視手段４０３から送信される制御データには、統計データ採取プログラム４０６の生成を指示する制御データ、そのプログラム４０６の起動（再開）を指示する制御データ、プログラム動作の終了を指示する制御データがある。

【００５３】統計データ採取プログラム動作監視手段４０３からの制御データが統計データ採取プログラム４０６の生成を指示するときは（ステップ８０３でＹＥＳ）、評価対象データ群生成手段１０１中の評価対象データ群２０４および統計プログラムライブラリ生成手段１０２の統計プログラムライブラリ３０３中の必要な統計プログラムに基づいて統計データ採取プログラム４０６を生成する（ステップ８０４）。そして、生成した統計データ採取プログラム４０６を起動し（ステップ８０６）、統計データ採取プログラム動作監視手段４０３からの制御データ受信待ちステップ８０２に戻る。

【００５４】統計データ採取プログラム動作監視手段４０３からの制御データがプログラム起動（再開）指示であるときは（ステップ８０５でＹＥＳ）、統計データ採取プログラム４０６を起動または再開し（ステップ８０６）、統計データ採取プログラム動作監視手段４０３からの制御データ受信待ちステップ８０２に戻る。

【００５５】統計データ採取プログラム動作監視手段４０３からの制御データがプログラム動作の終了指示であるときは（ステップ８０７でＹＥＳ）、必要な終了処理を行って自身を終了する（ステップ８０８）。

【００５６】図９を参照すると、統計データ採取プログラム中断・終了処理実行手段４０４は、動作を開始すると（ステップ９０１）、ステップ９０２～９０８の動作を実行する。まず動作開始後、統計データ採取プログラム動作監視手段４０３からの制御データ受信待ちを行い（ステップ９０２）、制御データを検出したら制御の指示内容を判定する（ステップ９０３，９０５）。統計データ採取プログラム動作監視手段４０３から送信される制御データには、統計データ採取プログラム４０６の中断を指示する制御データ、プログラム動作の終了を指示する制御データがある。

【００５７】統計データ採取プログラム動作監視手段４０３からの制御データが統計データ採取プログラム４０６の中断を指示するときは（ステップ９０３でＹＥＳ）、統計データ採取プログラム４０６がそれまでに採取し内部メモリに保持していたデータを統計結果格納手段１０６に格納できる中間データの形式に編集して統計結果格納手段１０６に格納すると共に、必要に応じて各種のメッセージ等を操作員へ表示する処理を行い（ステップ９０４）、統計データ採取プログラム４０６に対して中断指示を示す制御データを通知する（ステップ９０７）。そして、統計データ採取プログラム動作監視手段４０３からの制御データ受信待ちステップ９０２に戻る。

【００５８】統計データ採取プログラム動作監視手段４０３からの制御データがプログラム動作の終了指示であるときは（ステップ９０５でＹＥＳ）、統計データ採取プログラム４０６にプログラム終了指示を示す制御データを通知する等の処理を行い（ステップ９０６）、その後、自身を終了する（ステップ９０８）。

【００５９】図１０を参照すると統計データ採取プログラム４０６は、統計データ採取プログラム生成・起動（再開）手段４０５によって生成された後に起動されることにより動作を開始し（ステップＡ０１）、ステップＡ０２～Ａ０９の処理を実行する。

【００６０】まず起動後、制御データ受信検出を行う（ステップＡ０２）。このステップＡ０２で、所定時間内に統計データ採取プログラム中断・終了処理実行手段４０４からのプログラム中断指示や終了指示を検出したら（ステップＡ０３，Ａ０５）、それぞれステップＡ０４，Ａ０６へ進むが、統計データ採取プログラム生成・起動（再開）手段４０５からの起動（再開）を指示する制御データを検出するか、或いは何も検出しない場合は、ステップＡ０７へ進む。

【００６１】ステップＡ０７においては、評価データを

生成する。そして、その評価データを用いて評価対象プログラムの実行を行い（ステップＡ０８）、統計データを収集して一旦内部メモリに格納すると共に所定の時期に統計結果格納手段１０６に格納する（ステップＡ０９）。ここで、評価データの生成，統計データの収集と格納は、統計データ採取プログラムの一部として組み込まれた統計プログラムが担い、統計プログラムで生成された評価データが統計データ採取プログラムの一部として組み込まれた評価対象プログラムに引き渡されて出力データが生成され、この出力データと評価データとから統計プログラムが統計データを計算する。また、評価項目が複数設定されている場合、ステップＡ０７～Ａ０９による統計データの採取は評価条件で指定された評価項目順に行われる。さらに各評価項目においては、所定量の統計データを採取し終える毎に、制御データ受信検出ステップＡ０２に一旦戻り、このステップＡ０２において所定時間内に制御データが検出されない場合に残りの統計データの採取を続行すべくステップＡ０７～Ａ０９を実行する。

【００６２】ステップＡ０２において統計データ採取プログラムの中断指示の制御データを検出したときは（ステップＡ０３でＹＥＳ）、それまでステップＡ０７～Ａ０９で処理してきた評価項目について次回の再開に必要なプログラム再開用の情報を統計結果格納手段１０６に格納できる中間データの形式に編集して格納し（ステップＡ０４）、制御データ受信検出ステップＡ０２に戻り、このステップＡ０２において所定時間内に制御データが検出されない場合、未だ中断していない評価項目があれば次の評価項目に対しステップＡ０７～Ａ０９を実行する。全ての評価項目が中断していれば、ステップＡ０２でプログラム動作の再開を指示する制御データを待ち続け、再開指示を検出したらステップＡ０７に進んで最も過去に中断した評価項目についての処理を、その中断時点から再開する。

【００６３】ステップＡ０２において終了指示を検出したときは（ステップＡ０５でＹＥＳ）、統計データ採取プログラム動作監視手段４０３に終了通知を出す等の必要な終了処理を行って自身を終了する（ステップＡ０６）。

【００６４】図５を参照すると、統計結果編集出力手段１０５の一例は、数値処理手段５０３と、表形式数値データ編集出力手段５０５と、多次元グラフ編集出力手段５０６とを有している。

【００６５】表形式数値データ編集出力手段５０５は、統計結果格納手段１０６に格納された統計データ、つまり、評価対象となる暗号プログラムの入出力データのビットごとの相関関係を示す統計データを、表形式に編集して表示装置やプリンタ等に出力する手段である。

【００６６】多次元グラフ編集出力手段５０６は、統計結果格納手段１０６に格納された統計データを２次元若しくは３次元のグラフ形式に編集して表示装置やプリンタ等に出力する手段である。

【００６７】数値処理手段５０３は、統計評価システム制御手段１０３からの制御データに従って表形式数値データ編集出力手段５０５および多次元グラフ編集出力手段５０６を制御すると共に、統計結果格納手段１０６に格納された統計データに対して数値処理を施し、平均，最大，最小，分散，標準偏差等の基本統計量を求める手段である。なお、求められた基本統計量も表などと一緒に出力される。

【００６８】次に本実施の形態の暗号強度評価支援装置の動作を、暗号プログラムなどの具体例を挙げて詳細に説明する。なお、動作説明は以下の順に行う。

（１）前準備
（ａ）統計プログラムライブラリの準備
（ｂ）評価対象データ群の準備
（２）統計データの採取
（ａ）統計データ採取プログラムの生成と起動
（ｂ）統計データ採取プログラムの中断
（ｃ）統計データ採取プログラムの再開
（３）統計データの出力
（４）終了

【００６９】（１）前準備

暗号強度の評価を行う場合には、評価対象プログラム等を含む評価対象データ群２０４及び必要な統計プログラムを含む統計プログラムライブラリ３０３を事前に準備しておく必要がある。これらが既に準備されているときは、この段階は省くことができる。

【００７０】（ａ）統計プログラムライブラリの準備

統計プログラムライブラリ３０３中に必要な統計プログラムが存在しない場合、評価担当者は、統計プログラムライブラリ生成手段３０１を起動し、それが提供する環境の下で、基本機能ライブラリ３０２中の加算，減算，論理演算，平均計算等の基本的な演算機能を使って所望の統計プログラムを作成し、統計プログラムライブラリ３０３に追加する。以下の説明では、統計プログラムとして、ビットバランス用，出力ビット間関連用，入出力ビット間関連用，アバランシュ用の各統計プログラムが作成され、統計プログラムライブラリ３０３に格納されているものとする。

【００７１】（ｂ）評価対象データ群の準備

評価対象プログラムは評価対象プログラム作成手段２０１を使用して作成し、評価対象プログラムと統計プログラムとのインタフェースはインタフェース関数設定手段２０２を使用して設定し、評価条件は評価条件設定手段２０３を使用して設定する。

【００７２】図１１にＭｉｃｒｏｓｏｆｔ Ｖｉｓｕａｌ C++ 4.2を使って作成した評価対象プログラムの一例を示す。この例の評価対象プログラムでは、平文（ｔｅｘｔ）に鍵（ｍａｓｔｅｒｋｅｙ）を排他的論理和し

たものを暗号文（ｃｉｐｈｅｒ）とする暗号アルゴリズムの記述例になっている。

【００７３】図１２にＭｉｃｒｏｓｏｆｔ　Ｖｉｓｕａｌ　Ｃ++ 4.2を使って作成した評価条件の一例を示す。この例では、共通外部関数の宣言の形式で、採取する評価項目としてアバランシュ，ビットバランス，入出力ビット間関連，出力ビット間関連の４項目を指定している。また、統計プログラムが鍵およびデータを引き渡す領域も共通外部関数の宣言の形式で指定している。次に、外部変数宣言の形式で、鍵用乱数シード，入力データ用乱数シード，鍵のビット長，入力データブロックのビット長，出力データブロックのビット長，入力データ何回毎に鍵を変更するかを示す鍵変更回数，１つの鍵につき入力データを何回変更するかを示すデータ変更回数，何回計算するごとにキーボードの入力監視を行うかを示すキーボード入力監視間隔，何回計算するごとに計算結果を統計結果格納手段１０６にセーブするかを示す自動保存間隔を指定している。更に、外部関数宣言の形式で、評価対象プログラムを指定している。

【００７４】図１３にＭｉｃｒｏｓｏｆｔ　Ｖｉｓｕａｌ　Ｃ++ 4.2を使って作成した、評価対象プログラムと統計プログラムとのインタフェース関数の設定例を示す。この例では、統計評価用メイン関数としてａｖａｌａｎｃｈｅ（）；，ｉｏｒｅｌａｔｉｏｎ（）；，ｒｅｌａｔｉｏｎ（）；，ｂａｌａｎｃｅ（）；の合計４つが記述されている。これらは何れも統計プログラムであり、その実体は統計プログラムライブラリ３０３中にある。各統計評価用メイン関数はその記述順に実行される。各統計評価用メイン関数は、図１２中の外部変数宣言で指定された鍵用乱数シード，入力データ用乱数シードを使って鍵および入力データを発生し、図１２中の共通外部関数で指定された鍵およびデータの引き渡し領域に設定する。発生する鍵および入力データのビット長は，図１２中の鍵のビット長，入力データブロックのビット長に従う。また、図１２中の鍵変更回数，データ変更回数の指定に従って、発生する鍵および入力データを変更する。

【００７５】さらに図１３の例では、統計評価関数から鍵を受け取って評価対象プログラムに引き渡す関数や、統計評価関数から入力データを受け取って保存すると共に評価対象プログラムを呼び出して出力データを得る関数や、得られた出力データを保存する関数などが記述されている。統計評価関数はこれら保存された入出力データに基づいて統計データを計算し、最終的に統計結果格納手段１０６に出力する。

【００７６】（２）統計データの採取

（ａ）統計データ採取プログラムの生成と起動

操作員が統計データの採取を指示すると、統計評価システム制御手段１０３はその指示を認識し（図６のステップ６０３）、統計データ採取プログラム実行手段１０４に対してデータ採取開始を指示する制御データを送出する（ステップ６０４）。

【００７７】統計データ採取プログラム実行手段１０６の統計データ採取プログラム動作監視手段４０３は、上記のデータ採取開始を指示する制御データを認識すると（図７のステップ７０３）、統計データ採取プログラム４０６が未だ作成されていないので、統計データ採取プログラム生成・起動（再開）手段４０５に対してプログラム生成を指示する制御データを通知する（ステップ７０４）。

【００７８】統計データ採取プログラム生成・起動（再開）手段４０５は、上記のプログラム生成を指示する制御データを認識すると（図８のステップ８０３）、評価対象データ群生成手段１０１に準備されている評価対象データ群２０４と統計プログラムライブラリ生成手段１０２に準備されている統計プログラムライブラリ３０３中の必要な統計プログラムとを入力し、図１０に示したような動作を行う統計データ採取プログラム４０６を生成する（ステップ８０４）。この統計データ採取プログラム４０６の生成時に、図１１に例示したような評価対象プログラムと図１３に例示したようなインタフェース関数および統計プログラムライブラリ３０３中の統計プログラムとがリンクされ、１つの実行可能なプログラムが生成される。次に統計データ採取プログラム生成・起動（再開）手段４０５は、この生成した統計データ採取プログラム４０６を起動する（ステップ８０６）。

【００７９】生成され起動された統計データ採取プログラム４０６は、まず最初の評価項目に関して、評価データの生成（ステップＡ０７）、この生成された評価データを入力データとする評価対象プログラムの実行（ステップＡ０８）、評価データ及び評価対象プログラムの出力データに基づく統計データの収集と格納（ステップＡ０９）を行う。図１３の例では、統計評価用メイン関数がａｖａｌａｎｃｈｅ（）；，ｉｏｒｅｌａｔｉｏｎ（）；，ｒｅｌａｔｉｏｎ（）；，ｂａｌａｎｃｅ（）；の順に記述されているので、アバランシュ性評価データ，入出力ビット間関連性データ，出力ビット間関連性データ，バランス性データの順に、統計データの収集，保存が実行される。

【００８０】各評価項目のデータ収集は、図１２のキーボード入力監視間隔で指定された回数の計算毎に連続して行われ、指定された回数の計算が終了する毎に制御データ受信検出ステップＡ０２に一旦戻り、所定時間内に中断指示等がなければ、残りの計算を続行する。収集された各評価項目の統計データは、最終的には統計結果格納手段１０６に各評価項目別に格納される。

【００８１】（ｂ）統計データ採取プログラムの中断

操作員は統計データの採取中断を指示することで、現在実行中の評価項目についての処理を中断させ、次の評価項目の処理を開始させることができる。

【００８２】操作員が採取中断を指示すると、統計評価システム制御手段１０３はその指示を認識し（図６のステップ６０３）、統計データ採取プログラム実行手段１０４に対してデータ採取終了を指示する制御データを通知する（ステップ６０４）。

【００８３】統計データ採取プログラム実行手段１０６の統計データ採取プログラム動作監視手段４０３は、上記のデータ採取終了を指示する制御データを認識すると（図７のステップ７０５）、統計データ採取プログラム中断・終了処理実行手段４０４に対してプログラムの中断を指示する制御データを通知する（ステップ７０６）。

【００８４】統計データ採取プログラム中断・終了処理実行手段４０４は、上記のプログラム中断を指示する制御データを認識すると（図９のステップ９０３）、統計データ採取プログラム４０６がそれまでに採取し内部メモリに保持していたデータを統計結果格納手段１０６に格納できる中間データの形式に編集して統計結果格納手段１０６に格納すると共に、必要に応じて各種のメッセージ等を操作員へ表示する処理を行い（ステップ９０４）、統計データ採取プログラム４０６に対して中断指示を示す制御データを通知する（ステップ９０７）。

【００８５】統計データ採取プログラム４０６は、上記の中断指示を示す制御データを認識すると（図１０のステップＡ０３）、次回の再開に必要なプログラム再開用の情報を統計結果格納手段１０６に格納できる中間データの形式に編集して格納する（ステップＡ０４）。そして、制御データ受信検出ステップＡ０２に戻り、このステップＡ０２において所定時間内に制御データが検出されない場合、次の評価項目についてステップＡ０７～Ａ０９を実行する。

【００８６】（ｃ）統計データ採取プログラムの再開
操作員は全ての評価項目の処理が中断した場合、統計データの採取再開を指示することにより、中断した評価項目の処理をその中断時点から再開させることができる。

【００８７】操作員が採取再開を指示すると、統計評価システム制御手段１０３はその指示を認識し（図６のステップ６０３）、統計データ採取プログラム実行手段１０４に対してデータ採取開始を指示する制御データを送出する（ステップ６０４）。

【００８８】統計データ採取プログラム実行手段１０４の統計データ採取プログラム動作監視手段４０３は、上記のデータ採取開始を指示する制御データを認識すると（図７のステップ７０３）、統計データ採取プログラム生成・起動（再開）手段４０５に対してプログラム起動（再開）を指示する制御データを通知する（ステップ７０４）。

【００８９】統計データ採取プログラム生成・起動（再開）手段４０５は、上記のプログラム起動（再開）を指示する制御データを認識すると（図８のステップ８０５）、統計データ採取プログラム４０６に対して起動（再開）を指示する制御データを通知する（ステップ８０６）。

【００９０】統計データ採取プログラム４０６は、上記の起動（再開）指示を示す制御データを認識すると（図１０のステップＡ０５でＮＯ）、中断時点において統計結果格納手段１０６に格納してあった次回の再開に必要なプログラム再開用の情報を用いて動作を続行し、評価データの生成，評価対象プログラムの実行，データ収集・格納を続ける（ステップＡ０７，Ａ０８，Ａ０９）。このとき再開する評価項目は、最も過去に中断した評価項目である。

【００９１】以上のように本実施の形態では、現在実行中の評価項目についての処理を中断して次の評価項目を処理させることができる。１つの評価項目に関する統計データの収集には或る程度の時間がかかるので、この機能は、或る評価項目の処理を中断して次の評価項目を優先的に処理したい場合に便利である。なお、この機能をより実用的なものとするために、現在実行中の評価項目について、現在までの実行回数およびパーセンテージ，実行回数／秒，残り時間と終了時刻の予測値を算出して表示する機能を統計データ採取プログラム実行手段１０４に持たせるようにしても良い。この機能により、評価担当者は中断して良いか否かの或る程度の目安を得ることできる。

【００９２】図１４に表示装置にモニタ表示される統計データ採取プログラムの実行状況の一例を示す。この例では、操作指示をキーボード入力とし、起動（再開）指示はｅｎｃｒｉｐｔコマンドの入力で、中断指示は［ＥＳＣ］キーの押下で行うものとしている。また、［ＳＰＡＣＥ］キーを押下すれば、現在実行中の評価項目について、現在までの実行回数およびパーセンテージ，実行回数／秒，残り時間と終了時刻の予測値が表示されるようになっている。例えば図１４では、ｅｎｃｒｉｐｔコマンドの入力時、アバランシュ評価の開始メッセージが現在日時と共に表示されている。その後、［ＳＰＡＣＥ］キーが押下されており、第３，４行目に示されるように、現在実行中のアバランシュ評価項目について、現在までの実行回数（パーセンテージ，実行回数／秒），残り時間，終了時刻の予測値が表示されている。続いて［ＥＳＣ］キーが押下されており、アバランシュ評価が中断しその途中結果がセーブされたこと、次に入出力ビット関連評価の処理を開始した旨のメッセージが表示されている。

【００９３】（３）統計データの出力
操作員が編集形式など所定の項目を指定して統計データの編集出力を指示すると、統計評価システム制御手段１０３はその指示を認識し（図６のステップ６０５）、統計結果編集出力手段１０５に対して必要な制御データを通知する（ステップ６０６）。統計結果編集出力手段１

０５の数値処理手段５０３は、制御データを受信して解析し、必要な制御を実施する。

【００９４】例えば或る評価項目について、基本統計量と採取データの表形式との表示が指示された場合、数値処理手段５０３は統計結果格納手段１０６から当該評価項目の統計データを読み出して平均，最大，最小，分散，標準偏差等の基本統計量を求め、この求めた基本統計量と前記読み出した統計データとを表形式数値データ編集出力手段５０５に通知する。表形式数値データ編集出力手段５０５は、通知された統計データを所定の表形式に編集し、通知された基本統計量と共に表示装置やプリンタに出力する。表形式としては例えばＭｉｃｒｏｓｏｆｔ　Ｅｘｃｅｌ９７を使用することができる。

【００９５】図１５にＭｉｃｒｏｓｏｆｔ　Ｅｘｃｅｌ９７の表形式に編集して出力した表の例を示す。同図において、１５０１の部分が評価対象となる暗号装置の入出力データのビットごとの相関関係を示す統計データを表にしたもので、アバランシュ性評価データを例にしてある。この表の縦と横に記載されている０，１，２，…は一方が入力データのビット，他方が出力データのビットであり、その交点の数値が特定の入力ビットを反転した場合の特定の出力ビットの［反転回数－非反転回数］である。また、１５０２の部分は基本統計量を示し、平均，最大，最小，分散，標準偏差，９５％信頼区間が出力されている。なお、ｖａｌｕｅは値、ｘＳＤは（値－平均）÷σ，ｄｅｖｉａｔｉｏｎは偏差率，ｗｉｄｔｈは振れ幅である。その他、表には、鍵・入力データの乱数シード，予定していた全データ数，実行された全データ数などが記述されている。

【００９６】図１５のアバランシュ性評価データの表において、正の大きな数値は当該入力ビットと出力ビットとが高い相関性を持つことを示し、負の大きな数値は当該入力ビットが攪拌に役立っていないことを示し、何れも悪い性質を意味する。このようにデータ攪拌に偏りが発見された場合、そのアルゴリズムは選択差分を用いた攻撃などにより解読される可能性があり、強度的に弱いと言える。他方、絶対値の小さな数値は当該入力ビットの反転時に出力ビットが反転する確率が０.５に近いことを示し、攪拌性能が高いと言える。従って、絶対値の小さな数値の占める割合が多いほど暗号強度は強いと判定できる。従来の統計的な手法では基本統計量から評価しているが、例えば平均値を用いると、正や負の大きな数値が存在しても平均的には０に近くなる場合があり、評価を誤ることがある。また、特定の入力ビットと特定の出力ビットとの相関性を確認することができず、暗号化変換の挙動をきめ細かく把握することはできない。これに対し、表形式表示によれば暗号化変換の挙動をきめ細かく把握でき、正確な評価が行える。さらに、異なる評価対象プログラムについての表を見比べれば、異なる複数の暗号アルゴリズムの相対的な比較が容易に行える。これは、アバランシュ性評価に限らず入出力ビット間関連などの他の評価項目についても同じである。

【００９７】また、本実施の形態では、暗号装置の入出力データのビットごとの相関関係を示す統計データを２次元若しくは３次元のグラフ形式に編集して出力することもできる。２次元グラフの例としては、折れ線グラフ，等高線グラフなどがあり、３次元グラフの例としては、３Ｄ等高線などがある。このようなグラフ形式の指定は、統計評価システム制御手段１０３が例えば図１６に示すような「グラフ描画」ダイアログボックスを表示装置の画面に表示することで、グラフの種類の指定が容易に行える。図１６の例では、グラフの種類として、折れ線（系列：行），折れ線（系列：列），等高線，３Ｄ等高線，３Ｄ等高線（反転）の５種類が用意されており、操作員は描画したいグラフを選択し、ＯＫボタンを押すことで、編集するグラフの種類を簡易に指示できるようになっている。

【００９８】操作員から指示されたグラフの種類を指示するデータは、統計評価システム制御手段１０３から統計結果編集出力手段１０５に通知される。数値処理手段１０５は、或る評価項目について、編集するグラフの種類が指定されると、統計結果格納手段１０６から該当する評価項目の統計データを読み出して、グラフの種類を指定して多次元グラフ編集出力手段５０６に伝達する。

【００９９】多次元グラフ編集出力手段５０６は、指定されたグラフの種類に従って、統計データのグラフを例えばＭｉｃｒｏｓｏｆｔ　Ｅｘｃｅｌ９７の新規グラフシートに描画し、同時に表示装置またはプリンタにグラフを出力する。

【０１００】図１７に各グラフの表示例を示す。（ａ）が３Ｄ等高線、（ｂ）が３Ｄ等高線（反転）、（ｃ）が等高線、（ｄ）が折れ線（系列：行）、（ｅ）が折れ線（系列：列）である。

【０１０１】図１７（ａ）の３Ｄ等高線は、入出力データのビットごとの相関関係を「山」，「谷」，「平野」に模して描画したものである。例えばアバランシュ性評価データの場合、Ｘ軸に各入力ビットの目盛り，Ｙ軸に各出力ビットの目盛り、Ｚ軸に［反転回数－非反転回数］の目盛りを付け、［反転回数－非反転回数］の値が正方向に大きいほど「山」が高くなるように、負方向に大きいほど「谷」が深くなるように、絶対値が０に近いほど「平野」に近くなるように描画する。従って、高い山は入力と出力が高い相関性を持つことを、深い谷は相関性が極端に少ないことを示し、これらは何れも悪い性質を意味する。他方、平野は入力ビットの反転時に出力ビットが反転する確率が０.５に近いことを示し、良い性質を意味する。このような３Ｄ等高線を見れば、評価対象とする暗号アルゴリズム全体の挙動を直観的に素早く、細部まで漏れなく見渡すことが可能である。また、複数の評価対象プログラムの３Ｄ等高線を見比べれば、

異なる暗号アルゴリズムの相対的な比較が極めて容易に行える。

【０１０２】図１７（ｂ）の３Ｄ等高線（反転）は、同図（ａ）の３Ｄ等高線の山と谷を裏返しにしたものであり、３Ｄ等高線では見えにくい谷の様子を観察することができる。図１７（ｃ）の等高線は、同図（ａ）の３Ｄ等高線を図の①方向から見たもので、平野は薄く、山は濃く表示されている。図１７（ｄ）は同図（ａ）の３Ｄ等高線の任意の断面を同図の③の方向から見たときのグラフ、図１７（ｅ）は同じく３Ｄ等高線の任意の断面を④の方向から見たときのグラフであり、何れも３Ｄ等高線の細部をより詳しく観察する際に役立つ。

【０１０３】このように本実施の形態では、暗号装置の入出力データのビットごとの相関関係を３Ｄ等高線など種々のグラフで表示できるため、暗号変換の細部にわたる挙動をきめ細かく極めて容易に把握することができ、正確な評価が可能となる。

【０１０４】（４）終了

操作員が終了指示を入力すると、統計評価システム制御手段１０３はその指示を認識し（図６のステップ６０７）、統計データ採取プログラム実行手段１０４に対してプログラム動作の終了を指示する制御データを送出し、自身の動作を終了する（ステップ６０８）。

【０１０５】統計データ採取プログラム実行手段１０６の統計データ採取プログラム動作監視手段４０３は、上記のプログラム動作の終了を指示する制御データを認識すると（図７のステップ７０７）、統計データ採取プログラム中断・終了処理実行手段４０４および統計データ採取プログラム生成・起動（再開）手段４０５に対してプログラム動作の終了を指示する制御データを通知し、統計データ採取プログラム４０６から終了通知が出ると自身の動作を終了する（ステップ７０８）。

【０１０６】統計データ採取プログラム生成・起動（再開）手段４０５は、上記のプログラム動作の終了を指示する制御データを認識すると（図８のステップ８０７）、自身の動作を終了する（ステップ８０８）。また、統計データ採取プログラム中断・終了処理実行手段４０４は、上記のプログラム動作の終了を指示する制御データを認識すると（図９のステップ９０５）、統計データ採取プログラム４０６に対して終了指示を示す制御データを通知し（ステップ９０６）、自身の処理を終了する（ステップ９０８）。

【０１０７】統計データ採取プログラム４０６は、上記の終了指示を示す制御データを認識すると（図１０のステップＡ０５でＹＥＳ）、統計データ採取プログラム動作監視手段４０３に対して終了を通知し、自身の動作を終了する（ステップＡ０６）。

【０１０８】図１８は本発明の暗号強度評価支援装置の別の実施の形態の構成図である。この例の暗号強度評価支援装置は、中央処理装置およびメモリ等を備えたコンピュータ本体１８０１と、このコンピュータ本体１８０１に接続されたＣＲＴ１８０２，キーボード１８０３，マウス１８０４，磁気ディスク装置１８０５および記録媒体１８０６とで構成されている。記録媒体１８０６はＣＤ－ＲＯＭ，光磁気ディスク，半導体メモリ等の機械読み取り可能な記録媒体であり、暗号強度評価支援プログラムを記録してある。記録媒体１８０６に記録された暗号強度評価支援プログラムは、コンピュータ本体１８０１に読み込まれ、コンピュータ本体１８０１の動作を制御することにより、コンピュータ本体１８０１上に図１～図５に示した評価対象データ群生成手段１０１，統計プログラムライブラリ生成手段１０２，統計評価システム制御手段１０３，統計データ採取プログラム実行手段１０４，統計結果編集出力手段１０５をそれぞれ実現する。なお、図１の統計結果格納手段１０６は磁気ディスク装置１８０５で実現される。

【０１０９】以上本発明の実施の形態について説明したが、本発明は以上の実施の形態にのみ限定されず、その他各種の付加変更が可能である。例えば、評価対象となる暗号装置の暗号アルゴリズムが不明な場合、その暗号装置の入力データと出力データのデータ列から入出力データのビットごとの相関関係を求めるようにしても良い。この場合、評価対象データ群は、その暗号装置の入力データと出力データのデータ列から構成され、これらのデータ列から各評価項目データを採取する構成となる。

【０１１０】

【発明の効果】以上説明した本発明の暗号強度評価支援装置によれば以下のような効果を得ることができる。

【０１１１】特定の解読法に依存しないで暗号強度の評価が行える。その理由は、暗号装置の入出力データの相関関係に着目した統計的な評価を行うからである。このため、暗号アルゴリズムが不明でも、暗号装置の入出力データ列があれば評価が可能である。従来の評価、例えば線形解読法に必要な既知平文量で強度を評価しようとした場合、予め暗号アルゴリズムの線形近似式を求めなくてはならないが、暗号アルゴリズムが不明の場合には評価できない。具体的には、例えば、耐タンパー性をもった暗号装置の強度評価を行おうとした場合、本発明では実施可能だが、線形解読法に依存した評価方法は実施できない。

【０１１２】暗号化変換の挙動をきめ細かく把握することができる。その理由は、評価対象となる暗号装置の入出力データのビットごとの相関関係を示す統計データを表形式などに編集して出力するため、各ビットごとの相関関係を詳しく知ることができるからである。

【０１１３】暗号化変換の挙動が容易に把握できる。その理由は、評価対象となる暗号装置の入出力データのビットごとの相関関係を示す統計データを２次元若しくは３次元のグラフ形式に編集して出力するため、直観的な

把握が可能になるからである。

【０１１４】複数の暗号装置の暗号強度の比較が容易である。その理由は、複数の暗号装置の入出力データのビットごとの相関関係を示す統計データを同じ表形式や同じグラフ形式に編集して比較することにより、複数の暗号装置の挙動の細部を見比べることができるからである。

【０１１５】暗号装置の設計が効率的に行える。その理由は、暗号アルゴリズムの設計過程で、修正を行う前と後の暗号アルゴリズムの挙動の把握が容易になり、また相対的な強度比較が容易になったためである。また、評価対象プログラム作成手段を備えており、プログラムの修正から評価までを一連の作業として行うことができるためである。

【図面の簡単な説明】

【図１】本発明の暗号強度評価支援装置の実施の形態のブロック図である。

【図２】評価対象データ群生成手段の構成例を示すブロック図である。

【図３】統計プログラムライブラリ生成手段の構成例を示すブロック図である。

【図４】統計データ採取プログラム実行手段の構成例を示すブロック図である。

【図５】統計結果編集出力手段の構成例を示すブロック図である。

【図６】統計評価システム制御手段の動作例を示すフローチャートである。

【図７】統計データ採取プログラム動作監視手段の動作例を示すフローチャートである。

【図８】統計データ採取プログラム生成・起動（再開）手段の動作例を示すフローチャートである。

【図９】統計データ採取プログラム中断・終了処理実行手段の動作例を示すフローチャートである。

【図１０】統計データ採取プログラムの動作例を示すフローチャートである。

【図１１】評価対象プログラムの一例を示す図である。

【図１２】評価条件の一例を示す図である。

【図１３】評価対象プログラムと統計プログラムとのインタフェース関数の設定例を示す図である。

【図１４】表示装置にモニタ表示される統計データ採取プログラムの実行状況の一例を示す図である。

【図１５】統計データを編集して出力した表の例を示す図である。

【図１６】グラフの種類の指定に使う「グラフ描画」ダイアログボックスの例を示す図である。

【図１７】統計データを編集して出力した各種のグラフの例を示す図である。

【図１８】本発明の暗号強度評価支援装置の別の実施の形態の構成図である。

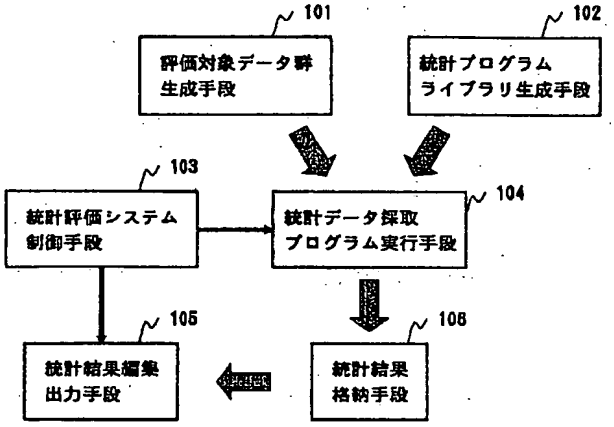
【符号の説明】

１０１…評価対象データ群生成手段
１０２…統計プログラムライブラリ生成手段
１０３…統計評価システム制御手段
１０４…統計データ採取プログラム実行手段
１０５…統計結果編集出力手段
１０６…統計結果格納手段
２０１…評価対象プログラム作成手段
２０２…インタフェース関数設定手段
２０３…評価条件設定手段
２０４…評価対象データ群
３０１…統計プログラムライブラリ生成手段
３０２…基本機能ライブラリ
３０３…統計プログラムライブラリ
４０３…統計データ採取プログラム動作監視手段
４０４…統計データ採取プログラム中断・終了処理実行手段
４０５…統計データ採取プログラム生成・起動（再開）手段
４０６…統計データ採取プログラム
５０３…数値処理手段
５０５…表形式数値データ編集出力手段
５０６…多次元グラフ編集出力手段

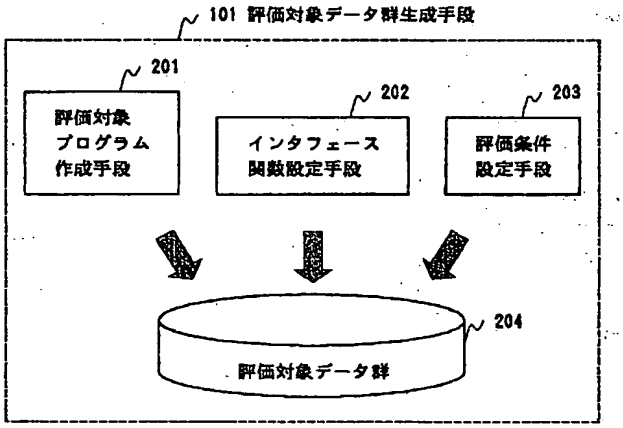
【図１１】

```
／＊暗号化アルゴリズムソースファイル＊／
／＊鍵と平文をＥＯＲし、暗号文とする（32bits/block）＊／
unsigned int masterkey;
void encript(unsigned int *test, unsigned int *cipher)
{
*cipher = *text ^ masterkey;
}
```

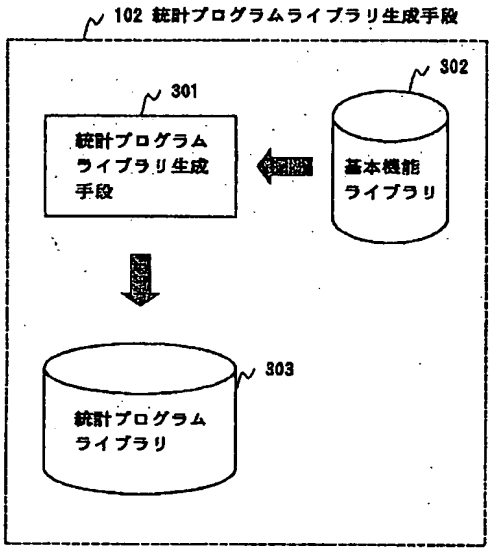
【図１】



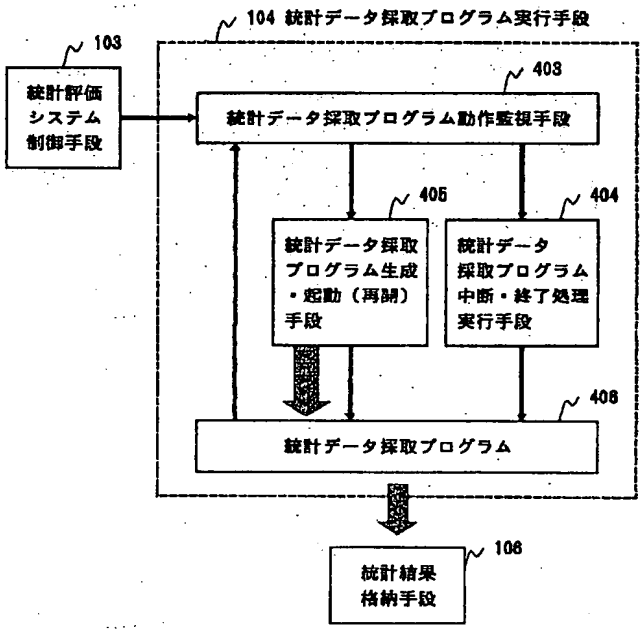
【図２】



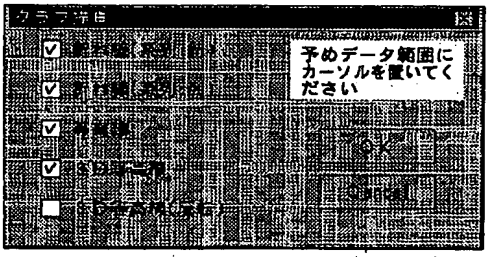
【図３】



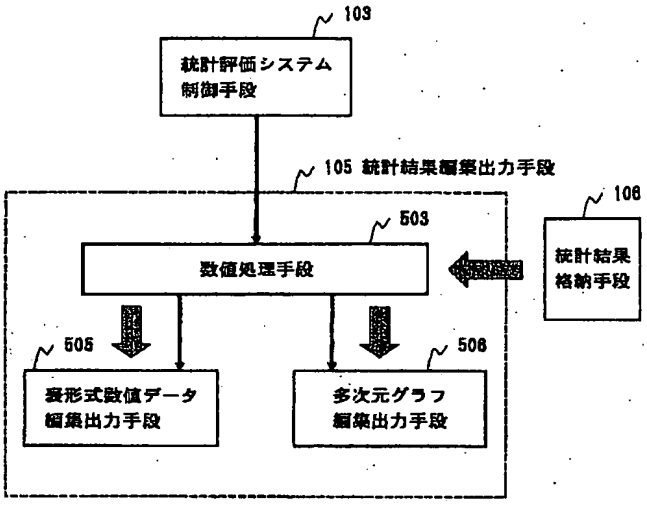
【図４】



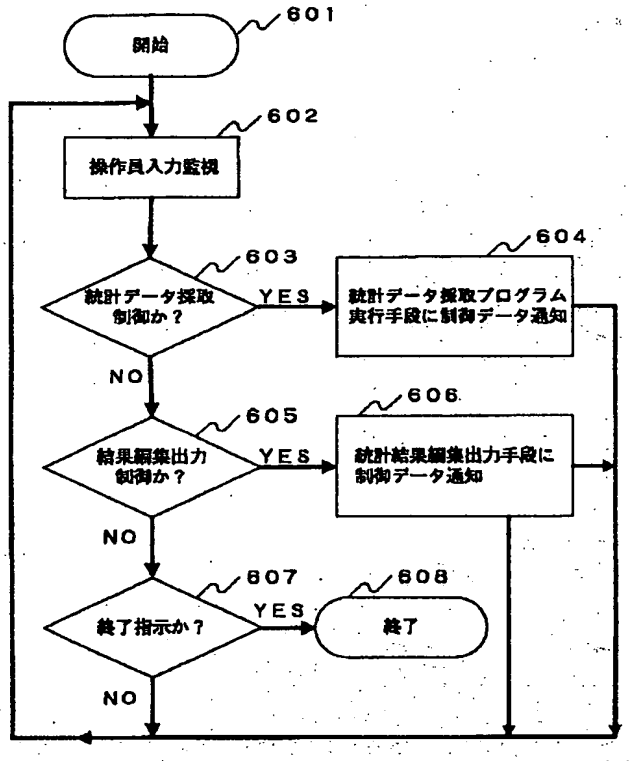
【図１６】



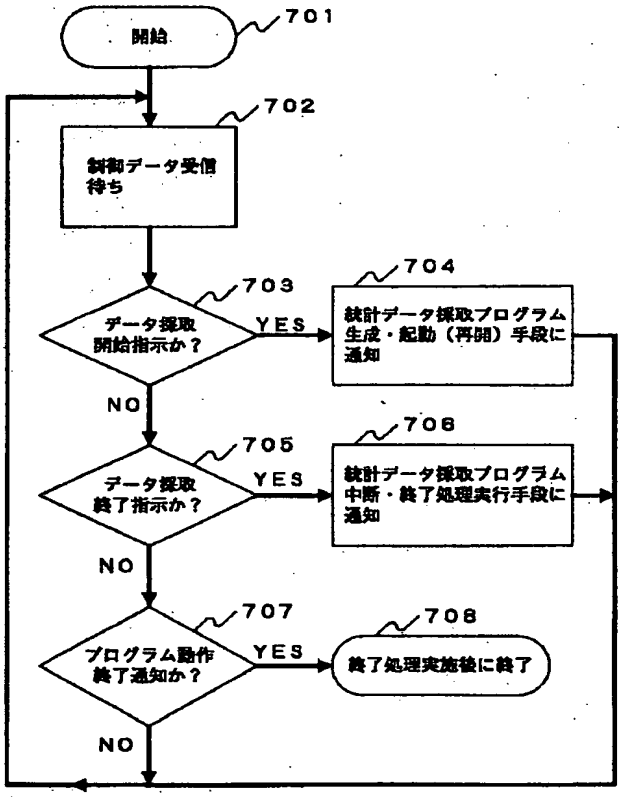
【図５】


103
統計評価システム制御手段
105 統計結果編集出力手段
106
統計結果格納手段
503
数値処理手段
505
表形式数値データ編集出力手段
506
多次元グラフ編集出力手段

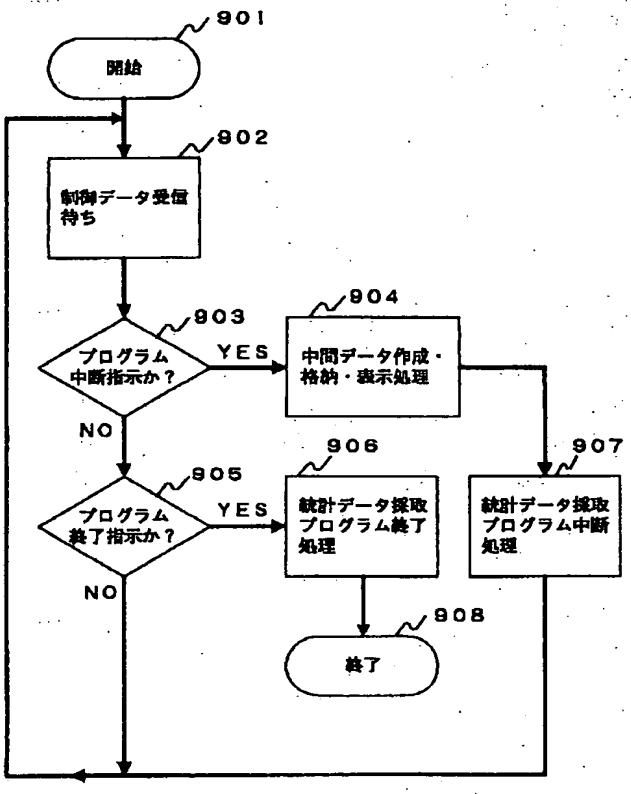
【図６】


601
開始
602
操作員入力監視
603
統計データ採取制御か？
YES
604
統計データ採取プログラム実行手段に制御データ通知
NO
605
結果編集出力制御か？
YES
606
統計結果編集出力手段に制御データ通知
NO
607
終了指示か？
YES
608
終了
NO

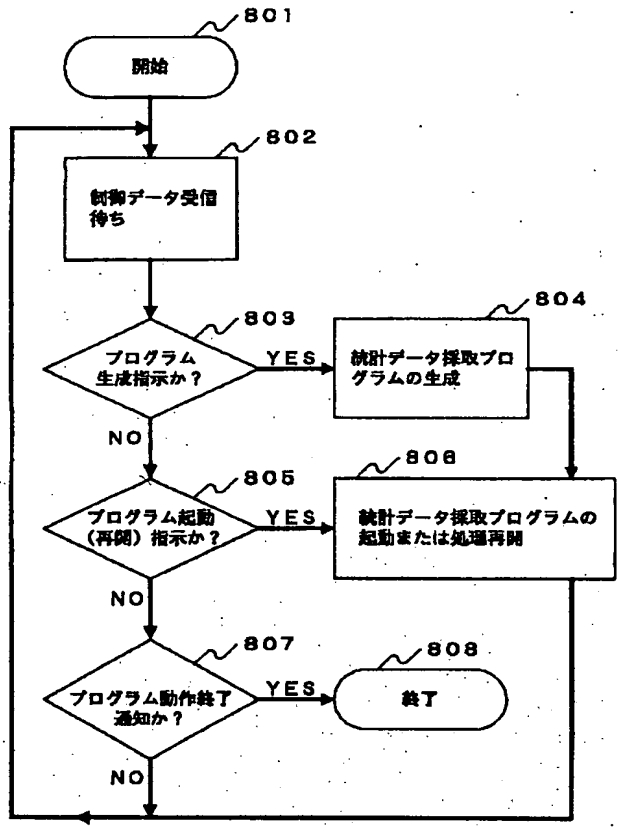
【図７】


701
開始
702
制御データ受信待ち
703
データ採取開始指示か？
YES
704
統計データ採取プログラム生成・起動（再開）手段に通知
NO
705
データ採取終了指示か？
YES
706
統計データ採取プログラム中断・終了処理実行手段に通知
NO
707
プログラム動作終了通知か？
YES
708
終了処理実施後に終了
NO

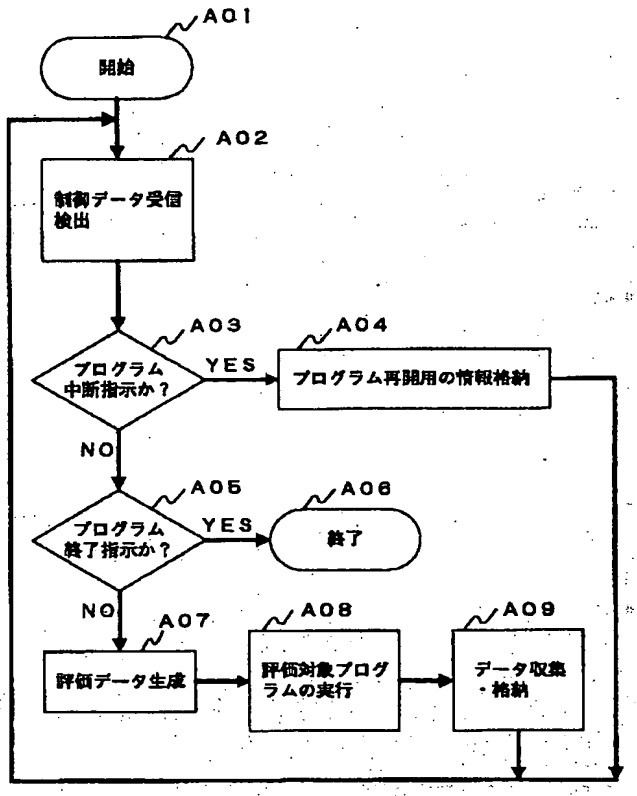
【図９】


901
開始
902
制御データ受信待ち
903
プログラム中断指示か？
YES
904
中間データ作成・格納・表示処理
NO
905
プログラム終了指示か？
YES
906
統計データ採取プログラム終了処理
907
統計データ採取プログラム中断処理
NO
908
終了

【図８】



【図１０】



【図１４】

```
B:¥Temp>encript
Avalanche(V4.0) test start! Fri Aug 08 14:46:28 1997
Avalanche(V4.0) Fri Aug 08 14:46:37 1997
Count =  2^14.322(0.24%  2276rps)---> [+1:01:17] Fri Aug 08 15:47:54 1997
SAVE: ava.sav RESULT: ava_last_.xls
Input/Output bit Relation(V4.0) test start! Fri Aug 08 14:46:43 1997
            :
            :
            :
            :
            :
B:¥Temp>encript
Avalanche(V4.0) test start! Fri Aug 08 14:47:40 1997
RESUME: ava.sav
            :
            :
            :
```

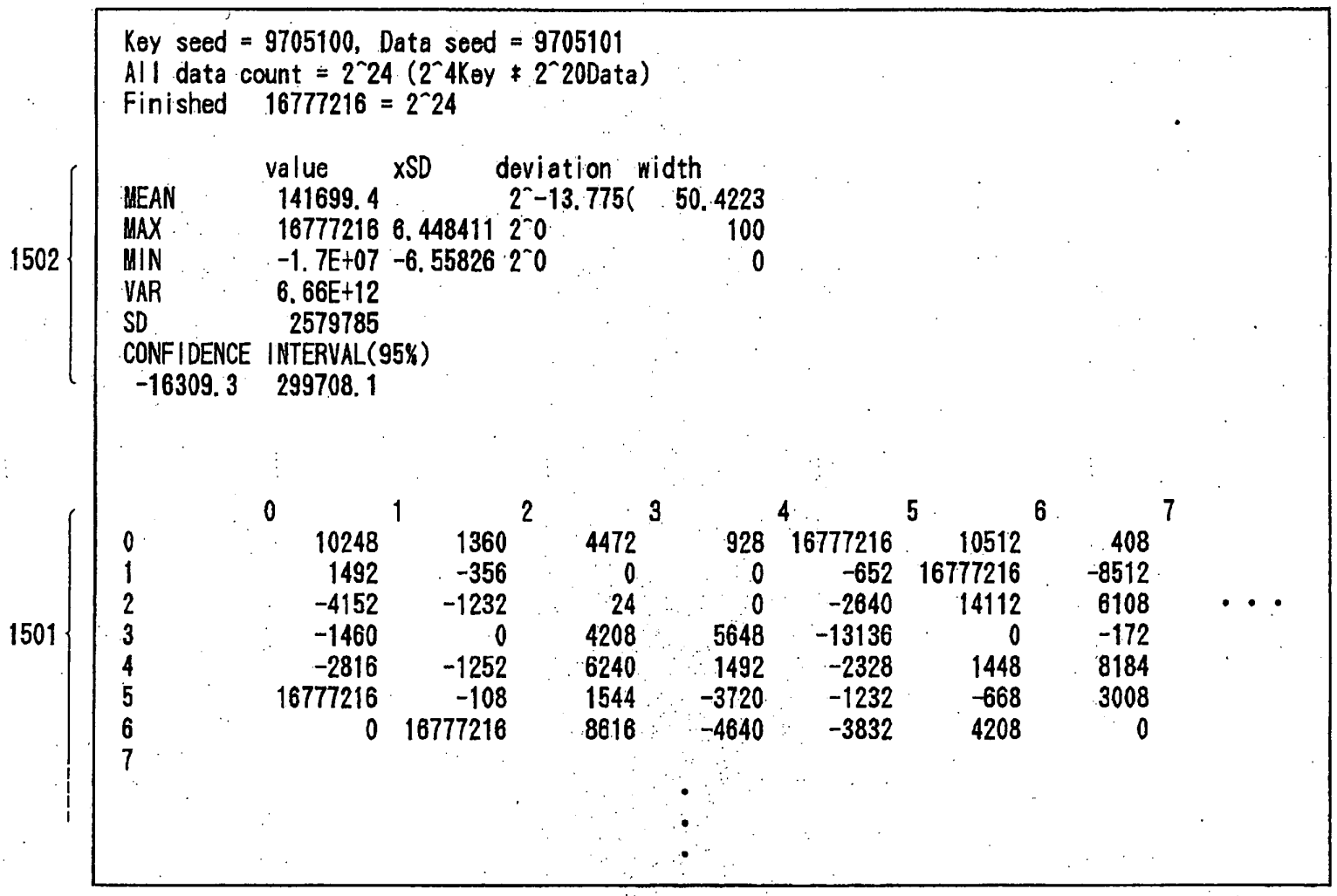
【図１２】

```
#include <conio.h>

／＊ユーザー定義型名＊／
typedef unsigned int uint;
typedef unsigned char uchar;

／＊共通外部関数＊／
void fKeyBlk(const uchar *);
void fDatBlk(const uchar *, uchar *);
extern void avalanche(void);
extern void balance(void);
extern void iorelation(void);
extern void relation(void);

／＊外部変数宣言＊／
uint dKeySeed = 9705150;  ／＊鍵用乱数シード＊／
uint dDatSeed = 9705151;  ／＊入力データ用乱数シード＊／
uint dKeyBit = 32;  ／＊鍵のビット長＊／
uint dInBit = 32; ／＊入力データブロックのビット長＊／
uint dOutBit = 32;  ／＊出力データブロックのビット長＊／
uint dKeyCnt = 6; ／＊鍵変更回数:  2^(dKeyCnt) 回変更する＊／
uint dDatCnt = 17;  ／＊データ変更回数: 1つの鍵につき 2^(dDatCnt) 回変更する＊／
uint dKbCnt = 12; ／＊キーボード入力監視間隔:  2^(dKbCnt)回計算毎に監視する＊／
uint dSavCnt = 31;  ／＊自動保存間隔:  2^(dSavCnt) 回計算毎に保存する＊／

／＊外部関数宣言＊／
extern void encript(unsigned int *, unsigned int *);
extern int key;
```

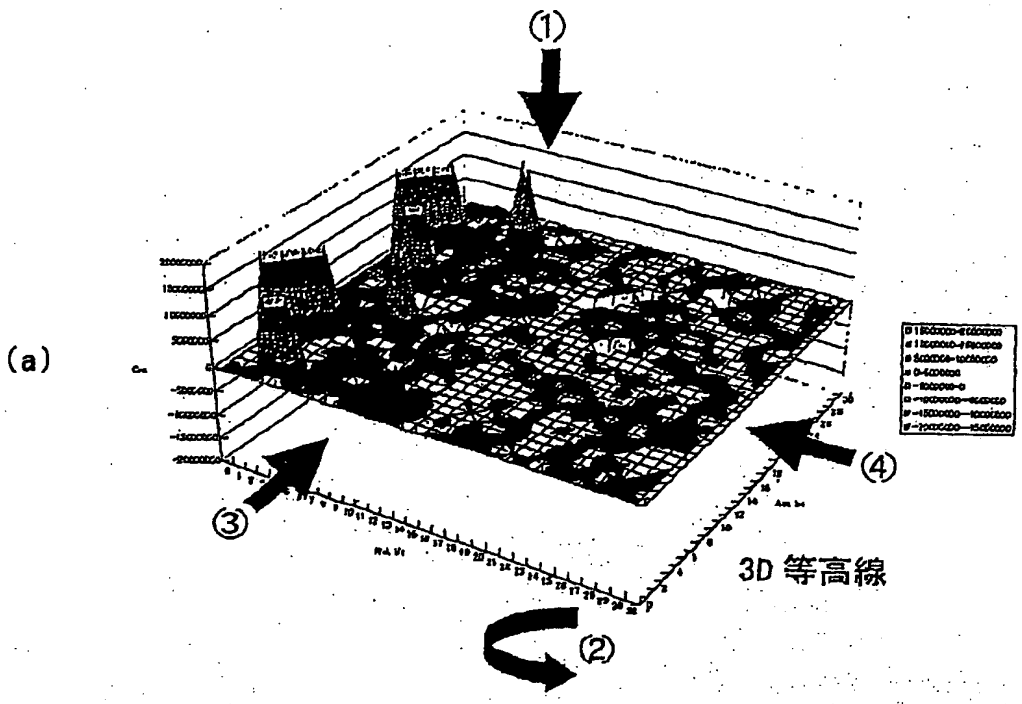
【図１３】

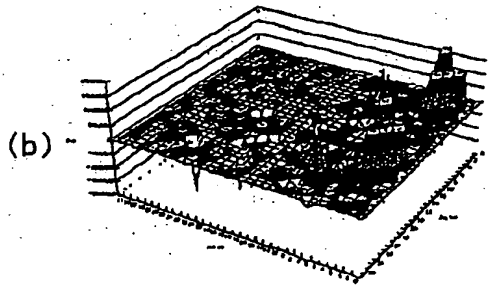
```
/*****************
 * main() 統計評価用メイン関数
 *****************/
void main(void)
{
/*統計評価関数を呼び出す*/
avalanche();  /*アバランシュ評価を実行する*/
iorelation(); /*入出力ビット間関連評価を実行する*/
relation();   /*出力ビット間関連評価を実行する*/
balance();    /*バランス評価を実行する*/
}

/*********************
 * fKeyBlk()  鍵を受け取って処理する
 *********************/
void fKeyBlk(const uchar *inkey)
{
masterkey =  inkey [0] <<24  | inkey [1] <<16  | inkey [2] <<8  | inkey [3] ;
}

/*****************************
 *  fDatBlk() データを受け取って評価対象データを作成する
 *****************************/
void fDatBlk(const uchar *indat, uchar *outdat)
{
uint text, cipher; /*入出力用ワーク変数の定義*/

/*入力用ワーク変数に indat [] の内容をコピーする*/
text = indat  [0] <<24  | indat [1] <<16  | indat [2] <<8  | indat [3] ;

/*評価対象を呼び出す*/
encript(&text, &cipher);

/*出力結果をoutdat [] にコピーする*/
outdat [0] = cipher>>24;
outdat [1] = cipher>>16;
outdat [2] = cipher>>8 ;
outdat [3] = cipher ;
}
```

【図15】

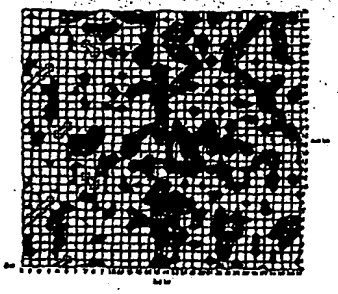

Key seed = 9705100, Data seed = 9705101
All data count = 2^24 (2^4Key * 2^20Data)
Finished 16777216 = 2^24
value xSD deviation width
MEAN 141699.4 2^-13.775(50.4223
MAX 16777216 6.448411 2^0 100
MIN -1.7E+07 -6.55826 2^0 0
VAR 6.66E+12
SD 2579785
CONFIDENCE INTERVAL(95%)
-16309.3 299708.1
1502
0 1 2 3 4 5 6 7
0 10248 1360 4472 928 16777216 10512 408
1 1492 -356 0 0 -652 16777216 -8512
2 -4152 -1232 24 0 -2640 14112 6108
3 -1460 0 4208 5648 -13136 0 -172
4 -2816 -1252 6240 1492 -2328 1448 8184
5 16777216 -108 1544 -3720 -1232 -668 3008
6 0 16777216 8616 -4640 -3832 4208 0
7
1501

【図１７】

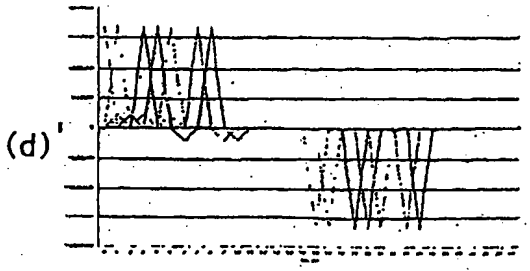




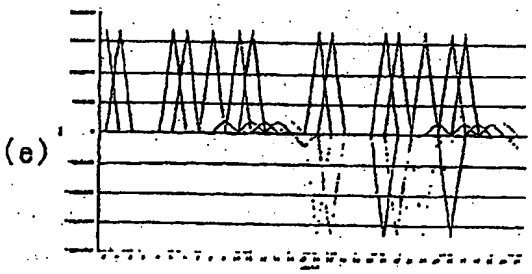
3D 等高線(反転) (②)



等高線 (①)

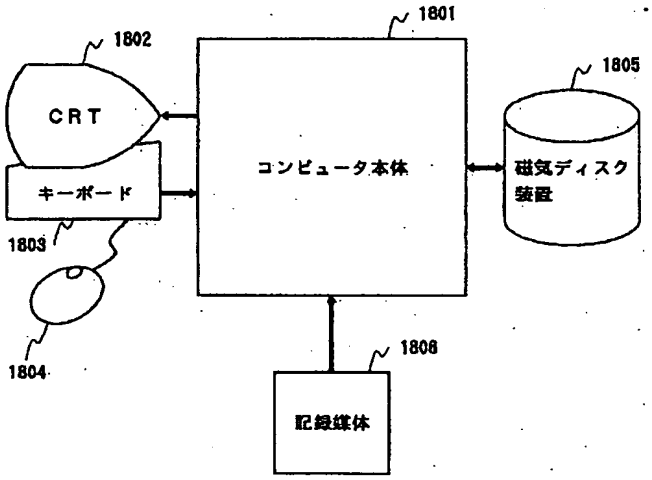


折れ線(系列:行) (③)



折れ線(系列:列) (④)

【図１８】


1801
1802
CRT
キーボード
1803
1804
コンピュータ本体
1805
磁気ディスク装置
1806
記録媒体